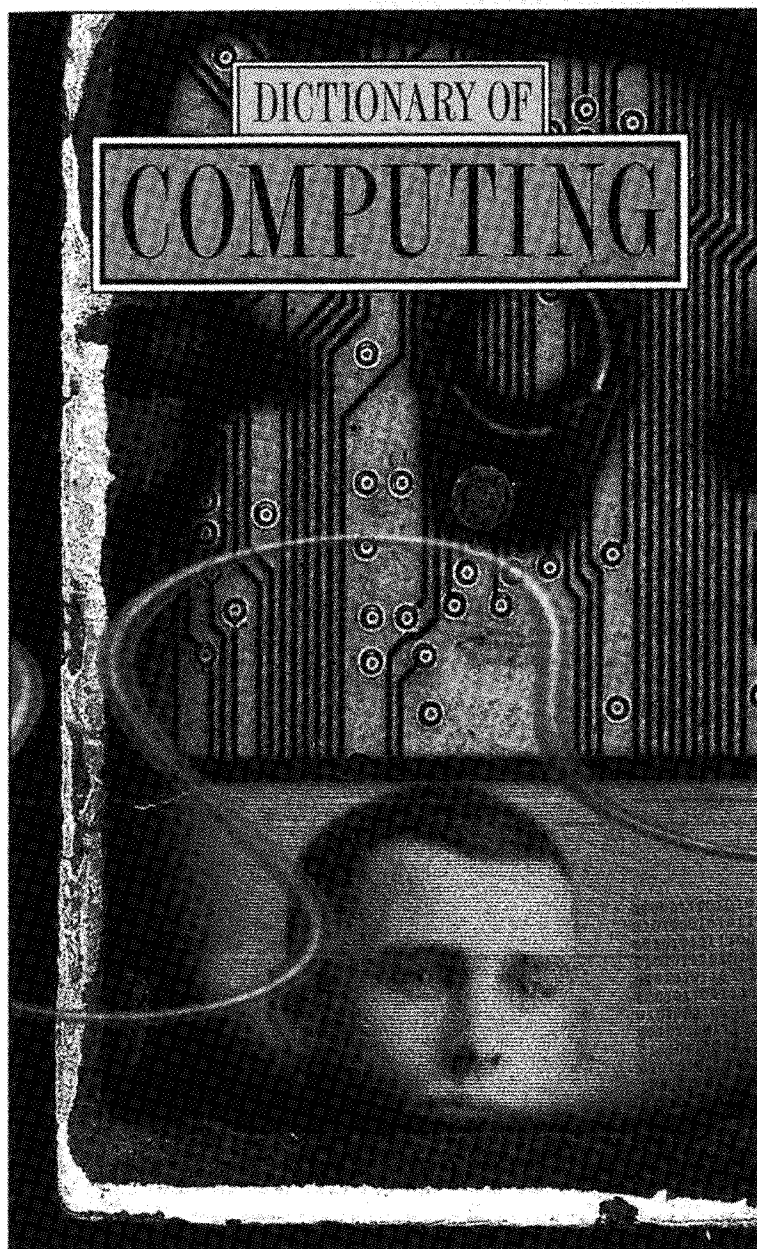


EXHIBIT M

O X F O R D

PAPERBACK REFERENCE



FOURTH EDITION

OXFORD PAPERBACK REFERENCE

A Dictionary of **Computing**

A Dictionary of
Computing

FOURTH EDITION

PERKINS COIE LLP

APR 09 2013

PALO ALTO LIBRARY

Oxford New York

OXFORD UNIVERSITY PRESS

1997

Oxford University Press, Great Clarendon Street, Oxford OX2 6DP

Oxford New York

Athens Auckland Bangkok Bogota Bombay Buenos Aires
Calcutta Cape Town Dar es Salaam Delhi Florence Hong Kong
Istanbul Karachi Kuala Lumpur Madras Madrid Melbourne
Mexico City Nairobi Paris Singapore Taipei Tokyo Toronto Warsaw
and associated companies in
Berlin Ibadan

Oxford is a trade mark of Oxford University Press

© Market House Books Ltd. 1983, 1986, 1990, 1996

First published 1983

Second edition 1986

Third edition 1990

Fourth edition 1996

First issued (with corrections) as an Oxford University Press paperback 1997

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior permission in writing of Oxford University Press. Within the UK, exceptions are allowed in respect of any fair dealing for the purpose of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act, 1988, or in the case of reprographic reproduction in accordance with the terms of the licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside these terms and in other countries should be sent to the Rights Department, Oxford University Press, at the address above

This book is sold subject to the condition that it shall not, by way of trade or otherwise, be lent, re-sold, hired out or otherwise circulated without the publisher's prior consent in any form of binding or cover other than that in which it is published and without a similar condition including this condition being imposed on the subsequent purchaser

British Library Cataloguing in Publication Data

Data available

Library of Congress Cataloging in Publication Data

Data available

ISBN 0-19-280046-9

1 3 5 7 9 10 8 6 4 2

Printed in Great Britain by

Biddles Ltd

Guildford and King's Lynn

CRYPTOLOGY

114

mitted. The recipient performs the reverse process with an identical pseudorandom sequence and the received ciphertext to recover the plaintext.

An alternative technique is to use a *block cipher, in which the ciphertext corresponding to each block of, typically, 64 bits of plaintext is generated algorithmically using a key. In a *symmetric* block cipher the key used for decryption is closely related to that used for encryption, and both have to be kept secret. With *asymmetric* or *public key encryption*, the decryption key cannot be deduced from knowledge of the encryption key, which can thus be publicized to all intending message senders. See Data Encryption Standard, RSA encryption.

cryptology The study of *cryptography.

c/s *Abbrev. for client/server.*

CSCW *Abbrev. for computer-supported cooperative working.*

CSG *Abbrev. for constructive solid geometry.*

CSL *Abbrev. for control and simulation language, one of the earliest *simulation languages. It is now obsolete.*

CSMA/CD *Abbrev. for Carrier Sense Multiple Access/Collision Detection, the formal name for *Ethernet.*

CSound A system for the programming of complex sounds and music. It has a number of different sound sources that may be combined together with a number of special effects. Typically a musician would create an orchestra file and a score file, the first defining the instruments in terms of the available sound sources and the second defining the performance of those instruments over time.

CSP *Abbrev. for communicating sequential processes. A mathematically formal approach to the description of software that addresses the specification of a set of concurrent processes and the way in which they interact; it was developed by Tony Hoare. The means of interaction is limited to a "synchronous" protocol in which any pair of communicating processes must be simultaneously involved for communication to be achieved.*

CSS *Abbrev. for centralized structure store.*

CTron *See Tron.*

CU *Abbrev. for control unit.*

CUA *Abbrev. for common user access. A specification created by IBM that defines the key-strokes and icon usage by which conforming applications implement frequently used activities, such as invoking menus or window sizing and positioning. For example, a *menu bar near the top of a window allows access to pull-down menus, which may be activated by a mouse or by typing Alt + F for the File menu, Alt + E for the Edit menu, etc. Also certain *buttons on the screen allow the user to minimize or maximize a window, select other applications, or reposition or resize a window.*

cubic spline A *spline curve of degree 3.

cull To remove objects from a complex *computer-graphics computation on the basis of a quicker test. For example, if the front faces of a cube are hidden by another object, all the geometry of the cube can be omitted from the calculation. See also back-face detection.

cumulative distribution function See probability distributions.

current address register Another name for program counter.

current instruction register (CIR) A register, usually in the control unit, that contains the information specifying the instruction that is being (or is about to be) performed. See also instruction format.

curried function A *function of one variable that is related to a function of several variables. Let f be a function of two variables, x and y . Then by considering x constant we obtain a function in y ; this function depends on the value of x . We write

$$g(x)(y) = f(x, y)$$

where g is called a curried version of f . Note that $g(x)$ denotes a function rather than a plain value. Curryng is often used in theoretical work to deal simply with functions of several variables, e.g. in the lambda calculus.

cursor A symbol on a display screen that indicates the active position, e.g. the position at which the next character to be entered will be displayed. The underline symbol is often used: it is made to blink or flash so that it is

easily noticed and can be distinguished from an underline that is part of the text. Other symbols, such as an arrow, pointing finger, or cross, are also used. The exact shape can be used to convey status information to the user. The cursor can be moved to a new position on the screen by means of *arrow keys on the keyboard or a *pointing device such as a mouse.

curvature In nonlinear *regression analysis, measures of curvature were proposed by D. Bates and D. Watts as a means of assessing the reliability of certain linear approximations. Curvature has two components: *parameter-effects curvature*, which can be reduced by suitable transformations of the parameters, and *intrinsic curvature*, which represents the essential aspect of nonlinearity. Estimation of these measures requires the second derivatives of the *expectation functions in the model.

curve compression Techniques for reducing the space needed to define complex curves.

cut 1. To mark a piece of text or graphical information in some way, read it into a temporary storage location, and delete it from the original document. The information may then be inserted into a new location. This has the effect of moving the information from one location to another and is often called a *move* or *cut and paste* by analogy with scissors and glue techniques. *See* clipboard. *Compare* copy.

2. A mechanism used in *Prolog to limit *backtracking. Roughly speaking, the effect of a cut is to fix certain decisions that have already been made, thus preventing the system from undoing those decisions in order to perform further search for solutions to its goals. This is a way of avoiding costly search known in advance to be fruitless, or of excluding alternative solutions that are not wanted. However, writing cuts in a program makes its behavior dependent on the system's search sequence. Such dependency prevents the program from being a pure statement of logical relationships and thus goes against the spirit of *logic programming.

cut and paste *See* cut.

cutout A portion of text or a graphic that has

been marked in some way, for instance by *dragging the cursor across it, in preparation for a *cut or *copy operation.

cut set of a *connected graph *G*. A set of edges whose removal produces a disconnected graph. *See also* connectivity.

cut-sheet feed *See* stationery.

cut vertex (articulation point) of a *connected graph *G*. A vertex of *G* whose removal together with the removal of all edges incident to it results in the remaining graph being disconnected. The term can also be extended and applied to more general graphs. Then the removal of a cut vertex and all arcs incident to it increases the number of connected components of the graph. *See also* connectivity.

CWIS *Acronym* for campus-wide information service. A specific form of information service dedicated to the needs of a campus, usually a university campus.

cybercafe A cafe equipped with terminals to provide public access to the *Internet.

cybernetics A discipline concerned with control and communication in animal and machine. Cybernetics attempts to build a general theory of machines independent of the material they are made from, e.g. electronic, organic, clockwork. Cybernetics draws an analogy between brains and electronic circuits. *See also* neural networks.

cyberspace An informal word first thought to have been used by the novelist William Gibson to refer to the total data on all the computers on all the networks in the world. The word has passed into common use as a way of referring to any large collection of network-accessible computer-based data.

cycle 1. (cycle time) An interval of time in which one set of events or phenomena is completed. It is usually the time required for one cycle of the memory system – the time between successive accesses – of a computer, and is sometimes considered to be a measure of *computer power.

2. Any set of operations that is repeated regularly and in the same sequence. The operations may be subject to variations on each repetition.